UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,179	03/05/2002	Handong Wu	NETAP020	7494

28875 7590 09/22/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/092,179	WU ET AL.	
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *06/11/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 have been examined.

Claim Objections

2. Claim 22 is objected to because of the following informalities: the claim is incomplete. Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-30 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

5. Claims 1 and 20 are directed to an intrusion detection method/system. The examiner respectfully asserts that the claimed method/system does not fall within the statutory classes listed in 35 USC 101. Thus, while the claimed invention may be labeled as a method/system it is in fact functional descriptive material (i.e., computer program, see specification page 16, line 15-page 17, line 5). Claims 1 and 20 are rejected as being functional descriptive material (i.e., computer program). Claims 2-19 and 21-29 depend on claims 1 and 20 and are rejected under the same rationale.

6. Claim 30 is directed to a computer program product for detecting intrusion. The examiner respectfully asserts that the claimed program product does not fall within the statutory classes listed in 35 USC 101. Thus, while the claimed invention may be labeled as a computer

program product, the computer-readable storage medium is a data signal (see specification page 17, lines 2-5). Claim 30 is rejected as being signal.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 3-11, 13-19 and 30 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya US Patent 6,279,113 B1.

9. As per claims 1 and 30, Vaidya teaches a method for detecting intrusion on a network, comprising:

storing signature profiles identifying patterns associated with network intrusion in a signature database [column 3, lines 27-38 and column 6, lines 35-42];

generating classification rules based on said signature profiles [column 3, line 65 – column 4, line 8];

receiving data packets transmitted on the network [column 6, lines 60-68];

classifying data packets having corresponding classification rules according to said generated classification rules [column 6, line 57 – column 7, line 10];

forwarding said classified packets to a signature engine for comparison with signature profiles [column 6, lines 63 – column 7, lines 5 and column 7, lines 11-21].

10. As per claims 3-9, Vaidya further teaches classifying said packets according to at least one packet field into groups [column 9, lines 46-61 and column 7, lines 2-21].

11. As per claims 10, 11, 13 and 14, Vaidya further teaches performing a table lookup to select an action to be performed on said packet based on its classification [column 7, lines 2-11 and column 9, lines 27-35].

12. As per claims 15 and 16, Vaidya further teaches partitioning signatures into disjoint groups to define subsets of signature profiles [column 6, lines 27-42].

13. As per claims 17-19, Vaidya further teaches filtering received packets and capturing packets at a network analysis device [column 8, lines 40-55].

14. Claims 20-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Copeland, III US Pub. 2002/0144156 A1 (hereinafter Copeland).

15. As per claim 20, Copeland teaches an intrusion detection system comprising:

A signature classifier comprising a first stage classifier operable to classify packets according to at least one packet field into groups and a second stage classifier operable to classify said packets within each of the groups according to a packet type or size [paragraph 0139, 0140 and 0165];

a flow table configured to support table lookups of actions associated with classified packets [paragraphs 0148, 0149];

a signature database for storing signature profiles identifying patterns associated with network intrusion [paragraphs 0020, 0153-0155]; and

a detection engine operable to perform a table lookup at the flow table select an action to be performed on said packet based on its classification, wherein comparing said packets to at least a subset of the signature profiles is one of the actions [paragraphs 0157 –0159 and 0163-0165].

16. As per claims 21 and 22, Copeland teaches the system further comprising a data monitoring device having a capture engine operable to capture data passing through the network and configured to monitor network traffic, decode protocols, and analyze received data [paragraph 0137].

17. As per claim 23, Copeland further teaches a parser operable to parse, generate and load signatures at the detection engine [paragraphs 0142-0146].

18. As per claims 24, Copeland further teaches the system comprising an alarm manager operable to generate alarms [paragraphs 0162-0164].

19. As per claims 25 and 26, Copeland further teaches a filter configured to filter out packets received at the intrusion detection system [paragraphs 0139-0141].

20. As per claim 27, Copeland further teaches the flow table is a hash table [paragraphs 0149-0150]

21. As per claims 28 and 29, Copeland further teaches action options listed in the flow table include dropping the packet and generating an alarm [paragraph 0165].

Claim Rejections - 35 USC § 103

22. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

23. Claims 2 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya US Patent 6,279,113 in view of Copeland US Pub. 2002/0144156 A1.

24. As per claims 2 and 12, Vaidya teaches the method as applied to claim 1 above. Vaidya is silent on the method comprising dropping data packets without corresponding classification rules. However, Copeland teaches an intrusion detection system including dropping data packets without corresponding classification rules [paragraph 0165]. Both Vaidya and Copeland teach a network intrusion detection system. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Copeland within the system of Vaidya in order to enhance the security of the system.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

September 16, 2005

SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100